

What is Claimed is:

Sub
A

1. A system for authorizing client access to a network resource, comprising:
at least one directory that can be accessed using a network protocol, said at least one
directory being configured to store information concerning an entity's organization; and
a firewall that is configured to intercept network resource requests from a plurality of
client users, said firewall being operative to authorize a network resource request based upon a
comparison of the contents of at least part of one or more entries in said at least one directory to
an authorization filter, wherein said authorization filter is generated based on a directory schema
that is predefined by said entity.

2. The system of claim 1, wherein said at least one directory is a lightweight
directory access protocol directory.

3. The system of claim 1, wherein said authorization filter is specified using a
graphical user interface.

4. The system of claim 1, wherein said authorization filter implements a per-user
authentication scheme.

5. The system of claim 1, wherein said authorization filter implements a per-service
authentication scheme.

6. The system of claim 1, wherein said firewall and said directory communicate using secure socket layer communication.

7. The system of claim 1, wherein said firewall is configured to query multiple
5 directories.

8. An authentication method at a firewall, comprising the steps of:

- (a) receiving a network resource request from a client user;
- (b) querying, using a network protocol, at least one directory that is configured to store information concerning an entity's organization, wherein said query is based upon an authorization filter that is generated based on a directory schema that is predefined by said entity;
- (c) determining, based on the results of said query, whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter; and
- (d) permitting said network resource request through said firewall if said
15 authorization filter is satisfied.

9. The method of claim 8, wherein step (b) comprises the step of querying said at least one directory using a lightweight directory access protocol.

10. The method of claim 8, further comprising the step of specifying an authorization
20 filter using a graphical user interface.

11. The method of claim 10, wherein said specifying step comprises the step of specifying an authorization filter that implements a per-user authentication scheme.

12. The method of claim 10, wherein said specifying step comprises the step of specifying an authorization filter that implements a per-service authentication scheme.

13. The method of claim 8, wherein step (b) comprises the step of querying said directory using secure socket layer communication.

14. The method of claim 8, wherein step (b) comprises the step of querying multiple directories.

15. The method of claim 8, wherein step (a) comprises the step of receiving a network resource request from a client user at an internal network.

16. The method of claim 8, wherein step (a) comprises the step of receiving a network resource request from a client user at an external network.

17. A computer program product for enabling a processor in a computer system to implement an authentication process, said computer program product comprising:

a computer usable medium having computer readable program code embodied in said medium for causing a program to execute on the computer system, said computer readable program code comprising:

first computer readable program code for enabling the computer system to receive a network resource request from a client user;

second computer readable program code for enabling the computer system to query, using a network protocol, at least one directory that is configured to store information concerning an entity's organization, wherein said query is based upon an authorization filter that is generated
5 based on a directory schema that is predefined by said entity;

third computer readable program code for enabling the computer system to determine, based on the results of said query, whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter; and

fourth computer readable program code for enabling the computer system to permit said
10 network resource request through said firewall if said authorization filter is satisfied.